МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

ЛИНЕЙНАЯ СЛОЖНОСТЬ И СЛУЧАЙНЫЕ СВОЙСТВА ПОТОКОВОГО ШИФРА WG-16

Жур Максим Анатольевич

Научные руководители:
проф. В. И. Громак,
проф. А. Потт

2014

Дипломная работа содержит:

- 71 страницу.
- 25 рисунков.
- 4 таблицы.
- 2 приложения.

Ключевые слова: *конечное поле, период, м-последовательность, примитивный многочлен, автокорреляция, алгоритм Берлекампа-Месси, постулаты Голомба, линейная сложность, дискретное преобразование Фурье, теорема Блэйхута.*

В дипломной работе рассмотрен потоковый шифр WG-16.

Целью дипломной работы являлось исследование и доказательство случайных свойств потокового шифра WG-16, а также анализ двух атак на потоковый шифр WG-16: атаки Берлекампа-Месси и атаки с помощью дискретного преобразования Фурье.

Для достижения цели использовались:

- теория конечных полей в кодировании.
- теория псевдослучайных последовательностей регистра сдвига с линейной обратной связью.
- алгебраическая теория кодирования.
- метод дискретного преобразовния Фурье над конечным полем.

В дипломной работе получены следующие результаты:

- доказаны случайные свойства потокового шифра WG-16: свойство большого периода, свойство баланса, свойство идеального распределения t-кортежей, свойство (идеальной) двухуровневой автокорреляции и линейная сложность.
- сформулировано и доказано свойство периода произведения многочленов.
- исследована взаимосвязь между числом линейной сложности и эффективностью атаки Берлекампа-Месси и атаки с помощью дискретного преобразования Фурье.

– реализован алгоритм атаки Берлекампа-Месси в пакете Wolfram Mathematica.

– построен и исследован ряд примеров, иллюстрирующих рассматриваемую теорию.

Новизна результатов дипломной работы состоит в доказательстве ряда практически важных свойств потокового шифра WG-16.

Дипломная работа носит теоретический характер. Ее результаты могут быть использованы в дальнейших исследованиях криптографических свойств псевдослучайных последовательностей, в рамках их практического применения в кодировании.

Все результаты дипломной работы строго доказаны в соответствии с принятыми в математике правилами. Обоснованность и достоверность полученных результатов обусловлена строгими математическими доказательствами сформулированных в работе теорем и следствий и согласованностью с результатами, известными ранее для конкретных частных случаев. Дипломная работа выполнена автором самостоятельно.

The diploma thesis contains:

- 71 pages.
- 25 pictures.
- 4 tables.
- 2 appendices.

Keywords: *finite field, period, m-sequence, primitive polynomial, autocorrelation, the Berlekamp-Massey algorithm, Golomb's postulates, linear complexity, discrete Fourier transform, Blahut's theorem.*

The diploma thesis describes WG-16 stream cipher.

The aim of the thesis was to study and prove the randomness properties of the WG-16 stream cipher WG-16, as well as the analysis of the two attacks on the WG-16 stream cipher: the Berlekamp-Massey attack and the discrete Fourier transform attack.

The following background knowledge was used:

- the theory of finite fields in coding.
- the theory of pseudo-random linear feedback shift register sequences.
- the algebraic coding theory.
- the method of discrete Fourier transform over a finite field.

In the the diploma thesis, the following results are obtained:

- the following randomness properties are proved: the long period property, the balance property, the ideal t-tuple distribution property, the (ideal) two-level autocorrelation property and linear span.
- the property of the period of the polynomials product was formulated and proved.
- investigated the relationship between the number of linear span and the efficiency of the Berlekamp-Massey attack and the discrete Fourier transform attack.
- The Berlekamp-Massey algorithm was implemented in Wolfram Mathematica.
- built and studied a number of examples to illustrate the proposed theory.

The novelty of the results of the thesis consists in proving a number of practically important properties of the stream cipher WG-16.

The diploma thesis is theoretical in nature. The results can be used in further studies of properties of cryptographic pseudorandom sequences in the context of their practical use in coding.

All results of the thesis rigorously proved in accordance with the rules of mathematics. Validity and reliability of the results is based on the strict mathematical proofs formulated in the theorems and corollaries and on the consistency with the results previously known for certain special cases.

The diploma thesis performed by the author independently.